

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with the following email address,
including information associated with the Microsoft
accounts of such address: Karltrujillo07308@outlook.com
that is stored at a premise controlled by Microsoft Online
Services, Custodian of Records, a company that accepts
service of legal process at One Microsoft Way, Redmond
WA 98052-6399.

Case No. 20-MJ-48

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. Sections 2423, 2251 and 2252.

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



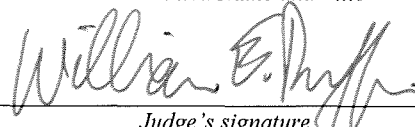
Applicant's signature

HSI Special Agent Kevin Wrona

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 2/19/2020



Judge's signature

City and State: Milwaukee, Wisconsin

Hon. William E. Duffin

U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kevin Wrona, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Special Agent Kevin Wrona has been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2010, and is currently assigned to the HSI Office of the Resident Agent in Charge (RAC) in Milwaukee, Wisconsin. SA Wrona has received training in the area of child pornography and child exploitation, and has had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, SA Wrona is a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and is authorized by law to request a search warrant.

2. SA Wrona makes this affidavit in support of an application for a search warrant to search the email accounts and associated cloud file hosting locations for information associated with certain accounts that are stored, owned, maintained, controlled, or operated by Microsoft, electronic communications services or remote computing services provider located at 1 Microsoft Way, Redmond, Washington 98052. The information to be searched consists of one (1) account (hereinafter, the Subject Accounts) and is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Attachment B.

3. The purpose of this application is to seize evidence more particularly described in Attachment B, of violation of 18 U.S.C. § 2252(a)(4)(B), which makes it a crime to knowingly

possesses, or knowingly accesses with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such a visual depiction involves the use of a minor engaging in sexually explicit conduct.

4. The statements contained in this Affidavit are based SA Wrona's experience and background as a SA with HSI, and by information provided by Wisconsin Department of Justice – Division of Criminal Investigation (DCI) SA Tamara Taubel. Some information in this affidavit also comes from information received from the issuance of administrative summonses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, SA Wrona has not included every fact known to him concerning this investigation. SA Wrona has set forth only the facts that he believes are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2423, 2251, and 2252 is located in the accounts described in Attachment A.

5. In SA Wrona and SA Taubel's training and experience, they have learned that Google, Yahoo, and Microsoft Outlook (hereafter "email providers") provide a variety of on-line services, including electronic mail ("e-mail") access, to the public. For example, Google allows subscribers to obtain e-mail accounts at the domain name "gmail.com," like the e-mail accounts listed in Attachment A; while Yahoo utilizes "yahoo.com." Subscribers obtain an account by registering with email providers. During the registration process, the email providers ask subscribers to provide basic personal information. Therefore, the computers of email providers

are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for subscribers) and information concerning subscribers and their use of services, such as account access information, e-mail transaction information, and account application information. In SA Wrona and SA Taubel's training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

6. An email subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by email providers, including Google Drive servers. In SA Wrona and SA Taubel's training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

7. In SA Wrona and SA Taubel's training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In SA Wrona and SA Taubel's training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

8. In SA Wrona and SA Taubel's training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of

service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

9. In SA Wrona and SA Taubel's training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In SA Wrona and SA Taubel's training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an

oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child pornography,” as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. “Cloud Storage” refers to saving data to an off-site storage system maintained by a third party. Instead of exclusively storing information to the computer’s hard drive or other local storage devices, the user saves it to a remote database (and or both). The Internet provides the connection between the computer and the database. There are several cloud-based storage options available to consumers (Dropbox, Google Drive, Box, Copy, Amazon, One Drive), with the majority of them offering gigabytes of storage free of charge.

d. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an

“e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

e. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

f. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

g. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

h. In describing image and video files, SA Wrona and SA Taubel frequently use the terms “pubescent” and “prepubescent.” SA Wrona and SA Taubel have no formal

medical training in the use of those terms but in applying them she relies on her experience as an investigator and her common experience. SA Wrona and SA Taubel use the term “pubescent” to mean a child who has begun to develop and display mature body shape and genital organs and/or secondary sexual characteristics such as, but not limited to, the development of breasts in females and the appearance of pubic hair and underarm hair. The term “pubescent” indicates her opinion that the person depicted is a child and evidences some physical and sexual maturation consistent generally with a young teenager or teenager. SA Wrona and SA Taubel use the term “prepubescent” to describe a child who does not exhibit any, or only very limited, physical-sexual development such as those indicators previously mentioned, such that the child appears to be well under the age of eighteen. The terms “toddler” and “very young child” should be given their common meanings and are used to communicate that the child depicted is clearly prepubescent and does not appear to be even nearing pubescence.

i. The terms “records,” “documents,” and “materials,” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

j. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

**BACKGROUND ON PEOPLE WITH AN INTEREST IN CHILD PORNOGRAPHY
AND ONLINE CHILD EXPLOITATION**

11. Based on SA Wrona and SA Taubel’s training and experience, as well as the training and experience of other law enforcement personnel with whom they have spoken, they have learned the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, videos, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography, but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer file sharing and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of individuals who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are

maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in computer storage devices, or in remote storage accounts.

d. Individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. One way to store child pornography without keeping the material on a specific device is to use cloud-based file storage services such as Google Drive, which can be accessed through an internet connection from any computer.

BACKGROUND ON NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

12. Based on SA Wrona and SA Taubel's training and experience, and publicly available information, they know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

13. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

14. The CyberTipline receives reports, known as CyberTips, about the possession, production and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

15. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b).

PROBABLE CAUSE

Initial Information Received from the National Center for Missing and Exploited Children (NCMEC)

16. On January 9th, 2020, Wisconsin Department of Justice – Division of Criminal Investigation (DCI) Special Agent (SA) Tamara Taubel was assigned the investigation regarding nine National Center for Missing and Exploited Children (NCMEC) CyberTipline reports. Five of the NCMEC CyberTipline reports were generated by Facebook, Inc. One report was generated by a citizen regarding the suspect's statements on Facebook. Two reports were generated by Twitter and one by Snapchat. SA Taubel reviewed each of those CyberTipline reports and associated files. SA Taubel summarized each of those CyberTipline reports.

17. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 39962623. The CyberTipline Report was submitted to NCMEC by Facebook. The following user uploaded two videos of suspected child pornography:

a. Name: Josh Nickel

Mobile Phone: +150531014XX

Date of Birth: 03-28-19XX

Approximate Age: 33

Email Address: jnickel6XX@gmail.com (Verified)

Screen/User Name: josh.nickel.1XX

ESP User ID: 1000132653714XX

Profile URL: <http://www.facebook.com/josh.nickel.1XX>

IP Address: 107.77.210.224 (Login) 09-06-2018 04:57:33 UTC

IP Address: 107.77.210.132 (Other) 09-08-2018 13:01:01 UTC

Email: jnickel6XX@gmail.com (Verified)

Mobile Phone: +150241768XX (Verified)

Mobile Phone: +133639024XX (Verified)

18. SA Taubel reviewed the two files and found that they were both the same video, which was consistent with child pornography. SA Taubel described that video below:

a. **Filename:**

**edik1vzj540kos0o41345750_1865261456900818_1100315358013220649
_n.mp4**

MD5: 8d0dcf847448db9ed0cc3b76391c2ba2

Submittal ID: e60645c182a327acc17c35ba945d39f

IP Address 107.77.210.132 Upload 09-08-2018 13:13:31 UTC

b. **Filename:**

**ekkk6zkerxkok88c41345750_1865261456900818_110031535801322064
9_n.mp4**

MD5: 8d0dcf847448db9ed0cc3b76391c2ba2

Submittal ID: 2a63417d22c9b02c3efcadacf6104453

Description: The video was one minute and thirteen seconds in length. The video was of a prepubescent Asian girl, with dark brown hair, laying on what appears to be a bed. The girl was not wearing any clothing. The video begins with a close camera view of the girl's lower torso area with her legs spread, exposing her vaginal area. In the lower portion of the video view was a Caucasian male erect penis being held by his right hand. The male was inserting his penis into the girl's anus. The male removed his penis from the girl's anus and ejaculated on her vaginal and anus areas. The girl was crying while this occurred. The male moved his ejaculate around the girl's vaginal area, with his fingers, and stated "stop stop. Stop stop stop. Bad bad bad. Bad bad." A female spoke to the girl in a language different than English.

19. Facebook provided information for the Facebook user that was sent and received the above video. SA Taubel included that information below:

a. **Filename:**

edik1vzj540kos0o41345750_1865261456900818_1100315358013220649_n.mp

4

MD5: 8d0dcf847448db9ed0cc3b76391c2ba2

Submittal ID: e60645c182a327acc17c35ba945d39f

IP Address 107.77.210.132 Upload 09-08-2018 13:13:31 UTC

Recipient:

First Name: Jon

Last Name: Curwood

Mobile Phone: +447849704349 (Verified)

Age: 37 DOB: 1980-10-31

Screen Name: jon.curwood.3

Profile Url: <http://www.facebook.com/jon.curwood.3>

IP Address: 31.49.250.220

IP Capture Date: August 25, 2018 at 10:01:55 UTC Uploaded September 8, 2018 at 06:13:31 PDT

20. SA Taubel queried the suspect's IP addresses, provided by Facebook, through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were AT&T Mobility. Those IP addresses were as follows:

a. 107.77.210.224 (Login) 09-06-2018 04:57:33 UTC – AT&T Mobility

107.77.210.132 (Other) 09-08-2018 13:01:01 UTC – AT&T Mobility

107.77.210.132 Upload 09-08-2018 13:13:31 UTC – AT&T Mobility

21. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 41181864. The CyberTipline Report was submitted to NCMEC by Facebook. The following user uploaded one video of suspected child pornography.

a. Name: Josh Nickel

Date of Birth: 03-28-19XX

Approximate Age: 33

Email Address: nascarfan2XX@gmail.com (Verified)

Screen/User Name: josh.nickel.581XX

ESP User ID: 1000231747770XX

Profile URL: <http://www.facebook.com/josh.nickel.581XX>

IP Address: 107.77.210.93 (Login) 10-03-2018 05:23:58 UTC

IP Address: 166.181.80.177 (Other) 10-03-2018 16:23:22 UTC

Additional Information: Estimated location on 10/04/2018 UTC: Lebanon, US
(Not Verified)

Email: nascarfan2XX@gmail.com (Verified)

22. SA Taubel reviewed the uploaded video and found it consistent with child pornography. SA Taubel described that video below:

a. **Filename:**

2xfr0z6qcn0g8kks43024177_2014745095259618_2367262803291465635

_n.mp4 MD5: d9207dda280b039afe09bc7a8a21bb1e

Submittal ID: 0ae1aec2ea12a63b0a6e7b55a9f8df7

IP Address 166.181.80.177 Upload 10-03-2018 16:49:15 UTC

Description: The video was one minute and fifty-nine seconds in length. The video was of a prepubescent Hispanic girl with long brown hair. The girl was not wearing any clothing and her vagina, breasts, and buttocks were exposed. The video was of the girl dancing in a seductive manner. At one point in the video a male stated something in a language different than English. The girl paused as if the male voice was giving her directions and then she began dancing again. While the girl was dancing, at points, the camera zoomed in on the girl's exposed vagina and exposed buttocks.

23. The video was sent to and received by the following Facebook user:

a. First Name: Mela

Last Name: Naka

Mobile Phone: +62882899778XX (Verified)

Age: XX

DOB: 19XX-09-30

Screen Name: mela.naka.X

Profile Url: <http://www.facebook.com/mela.naka.X>

IP Address: 115.178.212.145

IP Capture Date: October 4, 2018 at 08:27:20 UTC

Uploaded October 3, 2018 at 09:49:15 PDT

24. SA Taubel queried the suspect's IP addresses, provided by Facebook, through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were AT&T Mobility. Those IP addresses were as follows:

- a. 107.77.210.93 (Login) 10-03-2018 05:23:58 UTC – AT&T Mobility
166.181.80.177 (Other) 10-03-2018 16:23:22 UTC – Service Provider
Corporation
166.181.80.177 Upload 10-03-2018 16:49:15 UTC – Service Provider
Corporation

25. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 43129551. The CyberTipline Report was submitted to NCMEC by Facebook. The following user uploaded one image of suspected child pornography.

- a. Name: Joshua Nickel
Mobile Phone: +150520461XX
Date of Birth: 03-28-19XX
Approximate Age: XX
Screen/User Name: joshua.nickel.XX
ESP User ID: 1000282087656XX
Profile URL: <http://www.facebook.com/joshua.nickel.XX>
IP Address: 107.77.206.203 (Login) 11-12-2018 18:28:56 UTC

26. SA Taubel reviewed the uploaded image and found it consistent with child pornography. SA Taubel described that image below:

- a. **Filename:**
7cp4al4jytssoco446152853_278067356383486_6836188759441014784_n.jpg
MD5: 0d2546faeeca2cceaae90fa1305055ff
Submittal ID: 30e3d76947146b63d83347b5a018b7c
IP Address 107.77.206.203 Upload 11-13-2018 17:50:29 UTC

Description: The image was of a prepubescent Caucasian girl with long brown hair in braided pigtails. The girl was seated on a cream-colored chair. She was wearing a pink short sleeved shirt with a cartoon looking character on it and pink socks. The girl was not wearing any bottoms. Her legs were spread, bent at the knees, exposing her vaginal area. The girl was utilizing fingers from her right hand to touch her vagina. The focal point of the image appeared to be the girl touching her exposed vagina.

27. The user also uploaded an image as a profile photograph. That photograph was of a Caucasian male with a receding hairline and short brown hair. The male was smiling at the camera. He had a “scruff” looking mustache. The male was wearing a Green Bay Packers shirt and appeared to be wearing a black dog tag with a silver cross on it around his neck. The male was sitting on furniture which appeared maroon in color with a goldish colored floral pattern on it.

28. SA Taubel queried the suspect’s IP addresses, provided by Facebook, through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were AT&T Mobility. Those IP addresses were as follows:

a. 107.77.206.203 (Login) 11-12-2018 18:28:56 UTC – AT&T Mobility

107.77.206.203 Upload 11-13-2018 17:50:29 UTC – AT&T Mobility

29. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 53602361. The CyberTipline Report was submitted to NCMEC by Facebook. The following user uploaded one video of suspected child pornography.

a. Name: Joshua Nickel

Mobile Phone: +150520461XX (Verified)

Date of Birth: 03-28-19XX

Approximate Age: XX

Email Address: nascarfan1XX@yahoo.com (Verified)

ESP User ID: 1000092435166XX

Profile URL: [http://www.facebook.com/people/Joshua-](http://www.facebook.com/people/Joshua-Nickel/1000092435166XX)

Nickel/1000092435166XX

IP Address: 174.252.203.28 (Login) 08-12-2019 03:25:03 UTC

IP Address: 97.32.3.125 (Other) 08-13-2019 18:47:27 UTC

Email: nascarfan1XX@yahoo.com (Verified)

Email: Karltrujillo07308@outlook.com (Verified)

30. SA Taubel reviewed the uploaded video and found it consistent with child pornography. SA Taubel described that video below:

a. **Filename:**

**dihfliqzoxs08o8c69193502_2950659354950421_3542539197099462177
_n.mp4**

MD5: fe165bf8daad43305b6c94d376f50a40

Submittal ID: 4bcb15dfdd028b9a5bb2471fb32ea39e

IP Address 174.252.192.100 Upload 08-13-2019 19:46:15 UTC

Description: The video was forty-four seconds in length. The video was of a prepubescent Caucasian girl with blonde hair laying on her back on what appeared to be a bed. The blanket beneath the girl appeared to be green in color. The pillow had a green and blue design on it. The girl was not wearing any clothing and her vagina was exposed. A Caucasian adult male laying on his left

side on the right side of the girl. The male's upper thigh area, right hand, torso, upper left arm, and erect penis areas were in the view of the camera. The male stroked his penis towards the girl's vaginal area. The male ejaculated on the girl's vaginal and lower stomach areas.

31. The video was sent to and received by the following Facebook user:

a. First Name: Gary

Last Name: Anderson

Email: andre.gary19XX@gmail.com (Verified)

Age: XX

DOB: 19XX-01-30

Gender: Male

Profile Url: <http://www.facebook.com/people/Gary-Anderson/1000279190015XX>

Account ID: 1000279190015XX

IP Address: 2600:387:b:9::25

IP Capture Date: August 14, 2019 at 19:31:09 UTC

32. SA Taubel queried the suspect's IP addresses, provided by Facebook, through the American Registry for Internet Numbers (ARIN). The query showed that the provider of the IP addresses were Verizon Wireless. Those IP addresses were as follows:

a. 174.252.203.28 (Login) 08-12-2019 03:25:03 UTC – Verizon Wireless

97.32.3.125 (Other) 08-13-2019 18:47:27 UTC – Verizon Wireless

174.252.192.100 Upload 08-13-2019 19:46:15 UTC – Verizon Wireless

33. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 57547643. The CyberTipline Report was submitted to NCMEC by Twitter, Inc. The

following user uploaded files which, included suspected images of child pornography, to the user's account:

- a. Phone: +192020653XX

Screen/User Name: Josh544041XX

ESP User ID: 11766220985859645XX

Profile URL: <https://twitter.com/Josh544041XX>

- 34. SA Taubel reviewed the uploaded files and observed the following:

- a. **Filename: EHaFZdIXkAIh4-L.jpg**

MD5: 739650670ba97874daaf83eda8311a9d

Submittal ID: 839f8ed17e35dcd0cd53d08a2978a1be

Description: The image was of a young pubescent Caucasian girl, with light brown hair, seated on a dark surface with a white sheet as a background. The girl was wearing a white short sleeved shirt with "adidas" in pink lettering across the chest area. The girl was wearing white socks and black shoes. The girl's legs were spread and bent at the knees, with her hands holding the shin area of her legs. The girl's vagina was exposed and appeared to be the focal point of the image.

- b. **Filename: EHaN1bRWkAMi8Ms.jpg**

MD5: 9f7ae23e1dc2baef1d074166d05df404

Submittal ID: a9c8d42737e28063d7d80c5f29a0e032

Description: The image was of three Caucasian girls seated on a bed with a yellow, blue, pink, and green floral print on it. The girls were not wearing any clothing. The girl on the right was pubescent, had long brown hair, and had her right arm around the shoulder of the center girl. The girl on the right's right hand

was covering the center girl's right breast and her left hand was covering the girl's left breast. The center girl was pubescent and had long light brown hair. The girl on the left appeared to be early pubescent and had short dark blonde hair. She was seated with her legs crossed. The center girl's hand was on the left girl's right lower thigh area. The left girl's right breast was exposed. The focal point of the image appeared to be the posed nude girls.

c. **Filename: EHANx_nWwAAE9oN.jpg**

MD5: 7f897db7df23e2eb865a80023a226bcd

Submittal ID: 95d15de1ff885c3a7bb5e126dc731ef5

Description: The image was of two young prepubescent Caucasian girls with blonde hair. One girl was seated on a wooden chair and was wearing what appeared to be a pink short sleeved shirt and a red skirt. The girl was not wearing any underwear and her left leg was raised, exposing her vagina. The girl in pink had her arms around the other girl's neck/shoulder area. The second girl was wearing a blue short sleeved shirt and was on the right side of the girl in pink. The girl in blue shirt had her left pointer finger inserted into the girl's vagina, who was wearing pink. On the left cheek area of the girl in pink was an adult Caucasian male's erect penis. The male's penis was being held by his right hand. The majority of the male's body was outside of the frame of the photograph. Within the frame was his penis, right hand, a small part of his lower stomach, and the top part of his open blue jeans. The male was ejaculating into the open mouth of the girl in blue.

35. Within the uploaded files was a zip file entitled Josh54404111-1176622098585964549-2019-10-21-2122527. In the image section of the above file were many images. SA Taubel observed four images that she believed were consistent with child pornography. SA Taubel described those images below:

a. **File Name: 1186280074972151809-EHaDcPuW4AAXmm4**

Description: The image was of a late prepubescent Caucasian girl with light brown hair. The girl was seated on a dark colored surface with a blue background. The girl's hand were placed at the side and slightly behind her body, propping her body up. The girl was not wearing any clothing. The girl's legs were spread exposing her vagina. The girl's vaginal area appeared very red in color. There was a clear/white substance on the girl's stomach and vaginal area.

b. **File Name: 1186282226759192577-EHaFZdIXkAIh4-L**

Description: The image was of a young pubescent Caucasian girl, with light brown hair, seated on a dark surface with a white sheet as a background. The girl was wearing a white short sleeved shirt with "adidas" in pink lettering across the chest area. The girl was wearing white socks and black shoes. The girl's legs were spread and bent at the knees, with her hands holding the shin area of her legs. The girl's vagina was exposed and appeared to be the focal point of the image.

c. **File Name: 1186291446355316736-EHaNx_nWwAAE9oN**

Description: The image was of two young prepubescent Caucasian girls with blonde hair. One girl was seated on a wooden chair and was wearing what appeared to be a pink short sleeved shirt and a red skirt. The girl was not wearing any underwear and her left leg was raised, exposing her vagina. The girl in pink

had her arms around the other girl's neck/shoulder area. The second girl was wearing a blue short sleeved shirt and was on the right side of the girl in pink. The girl in blue shirt had her left pointer finger inserted into the girl's vagina, who was wearing pink. On the left cheek area of the girl in pink was an adult Caucasian male's erect penis. The male's penis was being held by his right hand. The majority of the male's body was outside of the frame of the photograph. Within the frame was his penis, right hand, a small part of his lower stomach, and the top part of his open blue jeans. The male was ejaculating into the open mouth of the girl in blue.

d. **File Name: 1186291502684741632-EHaN1bRWkAMi8Ms**

Description: The image was of three Caucasian girls seated on a bed with a yellow, blue, pink, and green floral print on it. The girls were not wearing any clothing. The girl on the right was pubescent, had long brown hair, and had her right arm around the shoulder of the center girl. The girl on the right's right hand was covering the center girl's right breast and her left hand was covering the girl's left breast. The center girl was pubescent and had long light brown hair. The girl on the left appeared to be early pubescent and had short dark blonde hair. She was seated with her legs crossed. The center girl's hand was on the left girl's right lower thigh area. The left girl's right breast was exposed. The focal point of the image appeared to be the posed nude girls.

36. In the folder titled 1176622098585964549-dm-media, SA Taubel observed a screen capture of a Twitter conversation between Josh @Josh54404111 and Elyssa @sincult19. That screen capture file name was 1185951910223851524-i4Iq4Glb. Josh was requesting "some

exclusive content of” Elyssa. Elyssa told Josh to “DM” her. Josh’s Twitter profile photograph was of a Caucasian male with short brown hair. The male had a receding hair line and a blue line under each eye.

37. In the file, 1186094468258246661-ZdnwblYu, SA Taubel observed a “selfie” style photograph of the same male was sitting in a vehicle with gray seats. The male was wearing a black and bright orange hooded sweatshirt. The male was wearing sunglasses.

38. Twitter, Inc. provided numerous IP addresses that had been utilized to login to the account. SA Taubel queried a selection of those IP addresses through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were Verizon, Charter Communications, and WiscNet. Three of those IP addresses were as follows:

- a. 216.56.8.220 (Registration) 09-24-2019 22:19:22 UTC – WiscNet
- 174.253.83.176 (Login) 10-21-2019 14:47:20 UTC – Verizon
- 174.102.129.190 (Login) 10-19-2019 15:55:40 UTC – Charter Communications

39. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 57619994. The CyberTipline Report was submitted to NCMEC by Twitter, Inc. The following user uploaded three files which, included suspected images of child pornography, to the user’s account:

- a. Email Address: bluefilm9XX@gmail.com
- Screen/User Name: Josh673120XX
- ESP User ID: 11862949790245765XX
- Profile URL: <https://twitter.com/Josh673120XX>

40. SA Taubel reviewed the uploaded files and observed the following:

a. **Filename: _i2z87be.jpg**

MD5: 609e2e82dbd5cf294b6ba7bef2e54609

Submittal ID: 196fd5d9af3a97f23b9b075ad8cf72db

Description: The image of a prepubescent Caucasian girl laying on her back. The girl was laying on what appeared to be a bed with gray blanket and white sheet with a grayish plaid pattern. The girl was wearing a light blue shirt and no bottoms. The girl's legs were raised in the air, bent at the knees, and spread, exposing her vagina and anus to the camera. There was a clear/white substance on the girl's anus/buttocks area. The girl was looking at the camera with a sad or in pain type look. The camera's focal point appeared to be the girl's anus/vagina area. The girl's face was visible through the center of her spread legs.

b. **Filename: h8p3jKRV.jpg**

MD5: 7f897db7df23e2eb865a80023a226bcd

Submittal ID: fffae729581b41a6c0fb3b22e5163121

Description: The image was of two young prepubescent Caucasian girls with blonde hair. One girl was seated on a wooden chair and was wearing what appeared to be a pink short sleeved shirt and a red skirt. The girl was not wearing any underwear and her left leg was raised, exposing her vagina. The girl in pink had her arms around the other girl's neck/shoulder area. The second girl was wearing a blue short sleeved shirt and was on the right side of the girl in pink. The girl in blue shirt had her left pointer finger inserted into the girl's vagina, who was wearing pink. On the left cheek area of the girl in pink was an adult Caucasian male's erect penis. The male's penis was being held by his right hand. The

majority of the male's body was outside of the frame of the photograph. Within the frame was his penis, right hand, a small part of his lower stomach, and the top part of his open blue jeans. The male was ejaculating into the open mouth of the girl in blue.

c. **Filename: Josh67312075-1186294979024576513-2019-10-22-2126829.zip**

MD5: 55fe6f5738d32874af7aff88c3b76531

Submittal ID: 4d73dbda3493fdac21a444a0770e4651

The above zip file contained numerous image and video files. Within those files SA Taubel observed one image that she believed to be consistent with child pornography. That image was described below:

Description: The image was of a late prepubescent Caucasian girl with light brown hair. The girl was seated on a dark colored surface with a blue background. The girl's hand were placed at the side and slightly behind her body, propping her body up. The girl was not wearing any clothing. The girl's legs were spread exposing her vaginal. The girl's vaginal area appeared very red in color. There was a clear/white substance on the girl's stomach and vaginal area.

41. Twitter, Inc. provided numerous IP addresses that had been utilized to login to the account. SA Taubel queried those IP addresses through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were Verizon, Wireless Data Service Provider Corporation, AT&T, and WiscNet. Three of those IP addresses were as follows:

a. 174.253.83.176 (Registration) 10-21-2019 14:55:45 UTC - Verizon

166.182.250.222 (Login) 10-22-2019 17:34:06 UTC – Wireless Data Service

Provider Corporation

174.253.85.245 (Login) 10-22-2019 15:54:30 UTC – Verizon

42. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 57873532. The CyberTipline Report was submitted to NCMEC by a citizen. The citizen reported that through the utilization of Facebook, they observed the following:

- a. "The post has since been removed however I witnessed an exchange between two members of the group where they were talking about being sexually interested in young girls. One member asked how old the youngest was that the other had ever have and mentioned that he had had relations with a seven year old. The other member mentioned that he was "Looking to find and bring one home today" Their facebook names are Josh Nickel from Watertown Wisconsin. His facebook claims he works for 7up Bottling company. The other has a facebook name of Jimbo Kinc. I believe this is a fake profile but this is the man who claims he has had relations with a seven year old. They have mentioned communicating with each other via facebook messenger as well."

43. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 58211494. The CyberTipline Report was submitted to NCMEC by Facebook. The following user uploaded two files which of suspected images of child pornography, to the user's account:

- a. Name: Josh Nickel
Date of Birth: 03-28-19XX
Approximate Age: XX
Screen/User Name: josh.nickel.52XX

ESP User ID: 1000403802010XX

Profile URL: <http://www.facebook.com/josh.nickel.52XX>

IP Address: 216.56.8.220 (Login) 10-24-2019 17:15:19 UTC

IP Address: 99.37.222.154 (Other) 10-25-2019 18:02:05 UTC

44. The NCMEC CyberTipline Report reported that both images were “identified as a match to a known child sexual exploitation image on NCMEC's NGO hash list.

45. SA Taubel reviewed the two images as described them below:

a. **Filename:**

**2fkuamk3n24g8o4w74346787_443521676273033_613206989678942617
6_o.jpg**

MD5: 9ad84613f96f1272516e8e53426e465e

Submittal ID: eb24113a2c7c858422be5b73d9855d3f

IP Address 99.37.222.154 Upload 10-25-2019 18:05:32 UTC

Description: The image of a prepubescent Caucasian girl laying on her back. The girl was laying on what appeared to be a bed with gray blanket and white sheet with a grayish plaid pattern. The girl was wearing a light blue shirt and no bottoms. The girl's legs were raised in the air, bent at the knees, and spread, exposing her vagina and anus to the camera. There was a clear/white substance on the girl's anus/buttocks area. The girl was looking at the camera with a sad or in pain type look. The camera's focal point appeared to be the girl's anus/vagina area. The girl's face was visible through the center of her spread legs.

b. **Filename:**

dkrp9slxezccgcs073498023_724652904665604_1873769050127990784_n.jpg

MD5: 8090dfd5f212ac768396fba7aaa501fd

Submittal ID: c4b47c5417cfe3b2b085a18ade127213

IP Address 99.37.222.154 Upload 10-25-2019 18:05:36 UTC

Description: The image was of two young prepubescent Caucasian girls with blonde hair. One girl was seated on a wooden chair and was wearing what appeared to be a pink short sleeved shirt and a red skirt. The girl was not wearing any underwear and her left leg was raised, exposing her vagina. The girl in pink had her arms around the other girl's neck/shoulder area. The second girl was wearing a blue short sleeved shirt and was on the right side of the girl in pink. The girl in blue shirt had her left pointer finger inserted into the girl's vagina, who was wearing pink. On the left cheek area of the girl in pink was an adult Caucasian male's erect penis. The male's penis was being held by his right hand. The majority of the male's body was outside of the frame of the photograph. Within the frame was his penis, right hand, a small part of his lower stomach, and the top part of his open blue jeans. The male was ejaculating into the open mouth of the girl in blue.

The above images were sent through Facebook to the following Facebook user:

c. First Name: Jimbo

Last Name: Kinc

Age: XX

DOB: 19XX-12-03

Gender: Male

Screen Name: jimbo.kiXX

Profile Url: <http://www.facebook.com/jimbo.kiXX>

Account ID: 1000413586809XX

IP Address: 222.155.78.97

IP Capture Date: September 18, 2019 at 03:59:10 UTC

46. Josh.nickel.52XX also uploaded an image of a Caucasian male with short brown hair. The male had a receding hair line and a blue line under each eye. Facebook reported that this image was the profile photograph for the Facebook account <http://www.facebook.com/josh.nickel.52XX>. SA Taubel reviewed this image and found that it was the same photograph as what was utilized as the profile photograph for a Twitter profile. That photograph was included in the information provided by Twitter, Inc. in CyberTipline Report 57547643. The following information for the user account was provided by Twitter in that CyberTipline Report:

a. Phone: +192020653XX

Screen/User Name: Josh544041XX

ESP User ID: 11766220985859645XX

Profile URL: <https://twitter.com/Josh544041XX>

47. SA Taubel queried the suspect IP addresses, provided by Facebook, through the American Registry for Internet Numbers (ARIN). The query showed that the IP address providers were WiscNet and AT&T. Those IP addresses were as follows:

a. 216.56.8.220 (Login) 10-24-2019 17:15:19 UTC – WiscNet

99.37.222.154 (Other) 10-25-2019 18:02:05 UTC – AT&T

99.37.222.154 Upload 10-25-2019 18:05:32 UTC – AT&T

99.37.222.154 Upload 10-25-2019 18:05:36 UTC – AT&T

48. SA Taubel was assigned the investigation regarding NCMEC CyberTipline Report 59240158. The CyberTipline Report was submitted to NCMEC by Snapchat. The following user uploaded five images of suspected child pornography:

a. Phone: +150241768XX

Date of Birth: 03-28-19XX

Email Address: jnickel6XX@gmail.com

Screen/User Name: jjnickel19XX

IP Address: 2600:1:930e:4944:9123:8ad:6778:27b0 11-12-2019 00:51:58 UTC

49. SA Taubel reviewed the uploaded files and observed the following:

a. **Filename: 07f47733-b3d8-4467-8bfc-**

5e9a19a05d18_CHAT_MEDIA_1573621077365.jpeg

MD5: d16211091fa8af3d31e8f3b278996d11

Submittal ID: 0b2ef0adda39267a6dad7f504be5fe

Description: The image was of a young prepubescent Caucasian girl with light brown hair. The girl was laying on her back on what appeared to be a blue blanket. The girl was not wearing any clothing. The girl's legs were spread, raised in the air, and bent at the knees. The girl's hands were on her buttocks/upper thigh area, on either side of her vaginal and anus areas. The girl's face was visible between her spread legs. The girl's vagina, anus, and breasts were exposed. The girl's exposed vagina and anus appeared to be the focal point of the image.

b. **Filename: 07f47733-b3d8-4467-8bfc-**

5e9a19a05d18_CHAT_MEDIA_1573621281229.jpeg

MD5: 8d0556d17f4c3039a9b3e62c3d170003

Submittal ID: e6dff5b1efaa15ef3b388dd177e8a47d

Description: The image was of three Caucasian girls seated on a bed with a yellow, blue, pink, and green floral print on it. The girls were not wearing any clothing. The girl on the right was pubescent, had long brown hair, and had her right arm around the shoulder of the center girl. The girl on the right's right hand was covering the center girl's right breast and her left hand was covering the girl's left breast. The center girl was pubescent and had long light brown hair. The girl on the left appeared to be early pubescent and had short dark blonde hair. She was seated with her legs crossed. The center girl's hand was on the left girl's right lower thigh area. The left girl's right breast was exposed. The focal point of the image appeared to be the posed nude girls.

- c. The following three image files were the same image:

Filename: 07f47733-b3d8-4467-8bfc-

5e9a19a05d18_CHAT_MEDIA_1573486025453.jpeg

MD5: dc4a2d0b4e1fd1b2aa950ec22f173f8b

Submittal ID: 8e2abce91b2be6967367587cd307a1f2

Filename: 07f47733-b3d8-4467-8bfc-

5e9a19a05d18_CHAT_MEDIA_1573500922571.jpeg

MD5: dc4a2d0b4e1fd1b2aa950ec22f173f8b

Submittal ID: 6e09a944a30d9006d847a52512cc7f5a

Filename: 07f47733-b3d8-4467-8bfc-

5e9a19a05d18_CHAT_MEDIA_1573621289132.jpeg MD5:

dc4a2d0b4e1fd1b2aa950ec22f173f8b

SA Taubel reviewed the above three image files and described them as follows:

The image was a of a young prepubescent Caucasian girl with shoulder length brown hair. The girl was laying on her stomach on a pink, purple, and green floral-patterned blanket. The girl was not wearing any clothing. An adult Caucasian male was kneeling, with his legs spread, straddling the girl's upper thigh area. The male was not wearing any clothing and his body from shoulders up was out of camera view. The male's hands were around the girl's waist and he appeared to be inserting his penis into the girl's anus.

50. SA Taubel queried the IP address 2600:1:930e:4944:9123:8ad:6778:27b0, provided by Snapchat, through the American Registry for Internet Numbers (ARIN). The query showed that the IP address provider was Sprint.

51. Wisconsin Department of Justice – Division of Criminal Investigation (DCI) Program and Policy Analyst (PPA) Dana Miller requested an administrative subpoena to Charter Communications, Inc. ordering information pertaining to 174.102.129.190 on 10/19/2019 at 15:55:40 UTC. The administrative subpoena was approved and signed by Assistant Attorney General (AAG) David Maas on November 19th, 2019.

52. That IP address was utilized to login to the Twitter account, <https://twitter.com/Josh544041XX>, on 10/19/2019 at 15:55:40 UTC. This information was provided in CyberTipline Report 57547643, which had been submitted by Twitter. In the CyberTipline Report, SA Taubel observed seven images of child pornography that had been uploaded to the account.

53. On November 20th, 2019, Charter Communications provided the requested

information. That information showed that the IP address subscriber during that time was the following:

a. Subscriber Name: MANAGEME CARDINAL CAPITAL

Subscriber Address: 4XX SUNNYSLOPE DR, HARTLAND, WI 53029-1420

User Name or Features: wschlossXX@cardinalcapital.us

Phone number: 262-367-28XX

Account Number: 7150191XX

MAC: a86badf1b7cb

54. A query of the address 4XX Sunnyslope Drive, Hartland, Wisconsin, through utilization of www.google.com, showed that the address was an apartment complex, Breezewood Village II. The apartment complex was run by Cardinal Capital Management, Inc. Listed under the property amenities was "Fee Wi-Fi."

CONCLUSION

55. DCI received nine National Center for Missing and Exploited Children (NCMEC) CyberTipline reports regarding, what was believed to be, the same suspect. Five of the NCMEC CyberTipline reports were generated by Facebook, Inc. One report was generated by a citizen regarding the suspect's statements on Facebook. Two reports were generated by Twitter and one by Snapchat. A total of twenty-two images of child pornography were uploaded to the suspect's social media accounts and/or shared with other users.

56. There were many similarities between the different reported social media accounts, which led SA Taubel to believe that it may be the same suspect utilizing each account. Both CyberTipline Reports 39962623 and 41181864 were both reported by Facebook. Both accounts utilized the same name, Josh Nickel, and date of birth, 03/28/19XX, for the user

information. In CyberTipline Report 43129551 the name was slightly different than the above two, listing Joshua Nickel as the user. The date of birth was again listed as 03/28/19XX. In CyberTipline Reports 43129551 and 53602361 the user utilized the same name of Joshua Nickel and the same telephone number of 505-204-61XX. In the account reported in CyberTipline Report 53602361, that telephone number was listed as verified. CyberTipline Report 57547643 was reported by Twitter and 58211494 was reported by Facebook. The Twitter account utilized IP address 216.56.8.220 on 9/24/2019 at 22:19:22 UTC to register their account. The same IP address was utilized by the Facebook account to login in 10/24/2019 at 17:15:19 UTC. Both accounts also utilized the same profile photograph. CyberTipline Report 39962623 was reported by Facebook and CyberTipline Report 59240158 was reported by Snapchat. Both users utilized the same telephone number for their accounts, 502-417-68XX. In the Facebook account, that telephone number was listed as verified. Both accounts also utilized the same date of birth as 3/28/19XX and email address of jnickel.6XX@gmail.com.

57. For a telephone number to be listed as verified, the user must follow instructions from the social media website to prove they have access to that telephone. For example, some social media websites will send a confirmation code to the telephone number and make them enter that code into the website or text back that code to the sending party.

58. In order to positively identify the suspect, SA Wrona and SA Taubel require additional records related to the social media accounts, and the related user information, listed in the CyberTipline Reports.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

59. SA Wrona anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and

2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications).

60. Based on the forgoing, SA Wrona requests that the Court issue the proposed search warrant.

61. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

63. SA Wrona requests that the Court order Microsoft not to notify any person (including the subscribers or customers of the account listed in Attachment A) of the existence of the requested warrant before August 12th, 2020, or until further order of the Court. Microsoft is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, SA Wrona seeks a warrant requiring Microsoft to disclose records and information in connection with a criminal investigation. This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant . . . is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant” *Id.*

64. Here, such an order is appropriate because the requested warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly,

there is reason to believe that notification of the existence of the requested warrant will seriously jeopardize the investigation, by giving the target an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an investigation. *See* 18 U.S.C. § 2705(b). The suspect is not aware of the investigation into him/her. If he/she were to learn the government is investigating him/her, he/she could destroy additional evidence of his/her crimes that may exist and be revealed during the search of his/her Microsoft account.

65. Based on the forgoing, SA Wrona requests that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A – Microsoft Outlook

Property to Be Searched

This warrant applies to information associated with the following email addresses, including information associated with the Microsoft accounts of such addresses:

- Karltrujillo07308@outlook.com

that is stored at a premise controlled by Microsoft Online Services, Custodian of Records, a company that accepts service of legal process at One Microsoft Way, Redmond WA 98052-6399.

ATTACHMENT B – Microsoft Outlook

Particular Things to be Seized

I. Information to be disclosed by Microsoft Outlook (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, for the time period of September 6, 2018 to the present, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, the contents, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail, and any/all attachments to such emails to include images and/or videos;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; all

records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

5. The Provider shall disclose responsive data, if any, by sending it to Special Agent Kevin Wrona, Homeland Security Investigations, 790 N. Milwaukee St., Suite 600, Milwaukee, WI 53202, kevin.c.wrona@ice.dhs.gov, using the US Postal Service, another courier service, or through email notwithstanding 18 U.S.C. 2252A or similar statute or code.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violation of 18 U.S.C. § 2252(a)(4)(B).